NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Chapter 13 IT System Security Planning

13.1 IT System Security Planning Overview

13.1.1 NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, provides the bulk of the guidance for preparing NASA's IT SSPs. NASA provides ITS-SOP-0016, Information Technology SSP, which fills in the gaps in the NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems that were caused by subsequent NIST publications.

13.1.2 All IT systems support NASA's enterprise architecture.

13.1.3 The purpose of an IT SSP is to:

a. Provide an overview of the system security requirements and pertinent risks and describe the controls that are planned for, or are already in place, that will result in cost-effective risk management and protection for the system and associated information.

b. Delineate the responsibilities and the expected behavior of all individuals who access the system or the information contained in the system.

c. Document the results of the security control selection and specification process, including justification and rationale for the final security controls selected and how the controls meet NASA's IT security requirements.

d. Provide the information system owner, the CA, and the AO the information necessary to make informed risk management decisions.

e. Contain requirements for various managers with responsibilities concerning the system, including information owners, the system administrator, and the system security manager.

13.1.4 The SSP is a critical document required as input for the security certification process that demonstrates that the controls designed and implemented for the system are adequate to protect NASA's information. Once the system has been certified, a NASA management official shall accredit the system prior to its going operational. The accrediting NASA AO assumes the risk of the system going operational and shall ensure that all controls have been validated by the CA. The accreditation of a system to process information provides an important quality control. (See Chapter 14, System Certification and Accreditation.)

13.1.5 IT SSPs will be grouped according to the guidance provided by the NASA SAISO, which can be found in Chapter 8, Master and IT Subordinate Systems.

13.2 IT System Security Plan Requirements

13.2.1 All master and subordinate system plans shall be developed using the ITS-SOP-0016, Information Technology SSP, for developing their SSPs. Since the SSP is a living document, sections shall be added to the plan or modified as the system matures.

13.2.2 The complete SSP, as developed and maintained by the information system owner, shall include:

a. SSP Executive Summary.

b. Document revision log.

c. Letter of accreditation.

d. Statement of Readiness for C&A.

e. Body of the SSP.

f. Attachments including, but not limited to, the acronym list, risk assessment documentation, contingency plan, interconnectivity agreements, POA&M, and other required documentation not included in the body of the SSP.

g. For MEI systems, a brief description of the rationale used for categorizing the system as an MEI along with the date that the OSPP approved the MEI determination.

13.2.3 All SSPs shall be protected as ACI or SBU information.

13.2.4 The SSP must be developed and reviewed for completeness prior to proceeding with the certification and accreditation process. Information system owners shall provide an acknowledgement statement that:

a. Indicates that the signers have reviewed the SSP and that it accurately reflects the system design, IT security strategy, the information's security category, risks that were accepted, and that the POA&M reflects the status of the tasks that need to be

accomplished to obtain full ATO.

b. Provides for the concurrence/non-concurrence signatures of the information system owner, information owners, lead CA, and SSP preparers.

c. Provides for the endorsement by the appropriate CIO, ITSM, and OSPP representative to proceed with the C&A process.

13.2.5 The SSP POA&M shall:

a. Identify tasks that must be accomplished prior to the system's being granted a full ATO.

b. Identify the resources required to accomplish each task.

c. Identify the milestones to be tracked in meeting the task.

d. Identify a schedule completion date for each milestone and task.

13.2.6 The Contingency Plan shall:

a. Summarize the requirements for continuity of critical operational processes and identify the individual responsible for the development and maintenance of the contingency plan.

b. See Chapter 15, System Contingency Planning, for complete guidance on contingency planning.

13.3 Additional IT System Security Plan References

a. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.

b. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

c. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS